MEDIA-INDEPENDENT DOCUMENT SECURITY METHOD AND APPARATUS

BACKGROUND

1. The Field of the Invention

This invention relates to document processing application software and, more particularly, to novel systems and methods for creating secure documents traceable to their origin, regardless of copying, and regardless of changes in media between copies. For example, a document may be copied onto a computer diskette, it may be printed to a printer, it may then be photocopied, it may then be scanned into a scanner to be restored in the memory of another computer.

2. The Background Art

Document security has been a difficult task from the inception of the written word. In a typical office, document security is often based on physical custody. Where a possibility exists for a document to be duplicated, certain means exist to render a duplicated copy unreadable.

For example, a document may be produced on a paper that contains a security mark such as the word "confidential" as a large, colored watermark. On a conventional copy machine, such as a photocopy machine, such a watermark turned black when copied. A black copy of a watermark, when a document was duplicated, was used to render the duplicate unreadable. Thus, this security method permitted only a single instance of a document, the original.

However, modern copier technology now allows copying of colors. Moreover with the advent of color copiers having the capacity for multiple shadings, conventional watermarks become inadequate.

A paperless office may present a different set of security issues. For example, an electronic document may be a "scanned" image of a paper document. Such a duplicate may be distributed to one or more individuals by a single keystroke. That is, with networks and internetworks connecting various computers, distribution may be massive with minimal individual effort. Moreover, any recipient of an electronic document may forward duplicates to an untold number of other individuals, some of whom may not be authorized to receive the document. Moreover, once a document has been duplicated, and distributed, electronic duplication may render more difficult the determination of a "leak" through which unauthorized documents were distributed.

To combat electronic security problems, many organizations, such as the United States Department of Defense (DOD), for example, prohibit transmittal of certain sensitive information by electronic mail. Other organizations attempt to control access to originals. Nevertheless, such an approach is rendered useless once an original document has been electronically sent to other individuals. Security as to all recipients of a document may be effectively impossible by conventional methods.

Other problems exist in electronic or paperless offices. For example, a recipient of a document may often "cut and paste" information received electronically. That is, most word processors and image processors, including drawing packages, drafting packages, and the like, permit editing of any or all portions of an electronic document.

To alter original documents, or fabricate new documents, is a simple matter of selecting certain editing tools and copying selected portions of the document received. Thus, editing may be virtually uncontrollable.

An internal office memo having an originator's initials written on it, for authentication purposes, may be dangerous.

For example, a recipient may scan a document into a computer using an image scanning device. The individual may then use a word processor or drawing application to "cut and paste" the image of the entire signature to be used at will. An individual may even fit or generate a piecewise function to re-create the signature at will.

Numerous efforts attempt to control the use and abuse of electronic signatures. Nevertheless, such efforts typically require a separate security file to be associated with an original document. If the security file is separated from the original, uncontrolled use of the signature may again be possible. Moreover, such separation may be extremely simple. One may print an original document with the electronic signature on it, scan the printed document back into a word processor or drawing processor, then "cut and paste" the signature to create a separate signature file. Transforming an original document from a paperless form to a hard copy or paper form effectively separates the original security files from the document itself. The original document may be rendered anew without any security file when scanned back into the computer hosting the word processor or drawing processor application.

Similarly, once a document has been misappropriated, improperly distributed, or the like, one of the improper copies may be located. Nevertheless, the source of the unauthorized copy is still not known. A pattern of unauthorized distribution may be difficult to locate or remedy.

What is needed is a document security system that is independent of the medium of transfer. That is, a document may be transferred on a wire, on an electromagnetic diskette, on a laser-encoded compact disk, on paper, on RAM, or the like. What is needed is a system in which transfer of a document by any medium, is incapable of removing security information from a resultant file.

BRIEF SUMMARY AND OBJECTS OF THE INVENTION

In view of the foregoing, it is a primary object of the present invention to provide a system for creating media-independent security for a document.

It is a further object of the invention to provide a processor programmed to execute instructions effective to create a document file and security instructions effective to create a security code, integrated into the document to be non-removable.

It is another object of the invention to provide a memory device operably connected to a processor for storing document files in a format to contain a substantive portion containing data corresponding to a readable image, a format portion corresponding to a layout of the document for outputting, and a security portion independent of the substantive portion and effective to be output as an integrated part of the document to be visually unreadable by human vision in a hard copy form.

It is another object of the invention to provide an input device for receiving an input signal corresponding to security data to be encoded into a document as an integrated portion thereof, in a security portion corresponding to the security code and unextractable from the document.

It is a further object to provide an output device operably connected to a processor to receive output signals corresponding to a document file such that the output device may render a document readable to a user as to substantive portion, while creating an independent security image unreadable to a user and yet effectively inseparable from the substantive portion in hard copy of the document.